University of Bahrain
IT College, Computer Science Department
ITCS 412: Cryptography and Network Security
Second Semester 2013/2014

Test II

Student ID	
Name	
Section	

This exam consists of **5** pages. Duration: One hour

	Part 1	Part 2	Part 3	Total
Maximum	10	20	10	40
Grade				

Part 1:

Answer the following questions by clearly circling the *most appropriate* answer [1 point each]

1. If public-key is used in message encryption, then encryption provides no confidence of sender since anyone potentially knows public-key. Is this statement true or false?

   a. True
   b. False

2. In public key encryption if A wants to send an encrypted message

   a. A encrypts message using his private key
   b. A encrypts message using B's private key
   c. A encrypts message using B's public key
   d. A encrypts message using his public key

3. A digital signature is required

   i. to tie an electronic message to the sender's identity
   ii. for non repudiation of communication by a sender
   iii. to prove that a message was sent by the sender in a court of law
   iv. in all e-mail transactions

   a. i and ii
   b. i, ii, iii
   c. iii, iv
   d. ii, iv

4. In public key encryption system if A encrypts a message using his private key and sends it to B

   a. if B knows it is from A he can decrypt it using A's public key
   b. Even if B knows who sent the message it cannot be decrypted
   c. It cannot be decrypted at all as no one knows A's private key
   d. A should send his public key with the message!

5. Hashed message is signed by a sender using

   a. his public key
   b. his private key
   c. receiver's public key
   d. receiver's private key

6. The responsibility of a certification authority (CA) for digital signature is to authenticate the

   a. hash function used
   b. private keys of subscribers
   c. public keys of subscribers
   d. key used in DES

7. For a 64-bit hash code, if birthday attack works, then how many trials on average needed to find another message with similar hash,

   a. 2^{33} trials
   b. 2^{64} trials
   c. 2^{63} trials
   d. $\sqrt{2^{64}}$ trials

8. Which of the following is **not** an SSL protocol

   a. SSL handshake protocol
   b. SSL change cipher Spec protocol
   c. SSL record protocol
   d. SSL session protocol

9. HTTPS refers to

   a. The HTTP and SSL handshake that allows the server and client to authenticate each other and to negotiate encryption
   b. The HTTP and SSL establishment of security capabilities by the client to initiate and establish capabilities
   c. The combination of HTTP and SSL to implement secure communication between a web browser and a web server.
   d. The HTTP-specific protocol to change of pending state to be copied into current state

10. Message Authentication Code (MAC) is a cryptographic checksum and is a _____ function.

a. One-to-one
b. One-to-many
c. Many-to-one
d. Many-to-many

Part 2:

1. Suppose that Alice chooses for an RSA system the primes $p = 31$, and $q = 43$, and the public key $e = 31$. [4 points]

   (a) Write the equation to encrypt the plaintext $M = 245$.

   (b) Write the equation to determine the private key d.

2. In RSA, what restriction that determine selecting the random number e in key generation? [1 points]

3. What is wrong with the following: Alice chooses for an RSA system the primes $p = 7$, and $q = 11$, and the public key $e = 5$ to encrypt message M=88. [1 points]

4. What is wrong with the following: Alice chooses for an RSA system the primes $p = 11$, and $q = 17$, and the public key $e = 8$ to encrypt message M=90. [1 points]

5. If Bob want to sign a message he encrypts the message using his private key [3 points]

   i. Prove that his approach is not correct. Assume Bob signed message m_1 and message m_2 then the signature for message m_1m_2 can be easily forged. Prove.

   ii. Find a solution to countermeasure previous attack.

6. If we have a hash function, how do we construct a MAC from it? [1 points]

7. Assume Alice and Bob shared their public keys. Now, Alice wants to send a secret message m to Bob and Bob can authenticate its from Alice. No hash functions used, only public keys. [2 points]

8. List four ways of distributing public keys. [2 points]

   i.

   ii.

   iii.

   iv.

9. What is a certificate authority? Explain a scenario in which they are useful. [3 points]

10. List two drawbacks for public key authorities [2 points]

Part 3:

1. In which layer of the TCP/IP protocol stack the SSL protocol is placed? and why it is not placed in the IP layer? [2 points]

2. What does *server_hello* message in phase 1 of SSL handshake protocol contain? [2 points]

3. What is the purpose of the dual signature in SET protocol? [2 points]

4. How can you prevent the following: [2 points]
   i. Replay attacks

   ii. Man-in-the-Middle attack in public key exchange

5. Explain how certificates get revoked. [2 points]